REMARKS

Claims 58-63 have been added. Therefore, claims 1-63 are pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Objection to the Title:

The Examiner objects to the title as not being descriptive and indicative of the invention to which the claims are directed. The Examiner suggests adding "CORBA" to the title. Applicants submit that the present title, "Secure Access to Managed Network Objects using a Configurable Platform-Independent Gateway" is descriptive and indicative of the invention to which the claims are directed. Furthermore, since the invention is not limited to only CORBA embodiments, adding the word "CORBA" to the title would in fact misrepresent the present invention.

Section 102(e) Rejection:

The Office Action rejected claims 1-57 under 35 U.S.C. § 102(e) as being anticipated by Barker et al. (U.S. Patent 6,363,421) (hereinafter "Barker"). Applicants respectfully traverse this rejection in light of the following remarks.

Regarding claim 1, Applicants respectfully disagree with the Examiner's interpretation of Barker and submit that Barker does not anticipate a gateway that is configurable to provide object-level access control between the managers and the managed objects, wherein said object-level access control is provided at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects. Instead, Barker discloses a system for "access control based on client name and password" (Barker, column 8, lines 45-46). Barker describes this as "a method of *client based* access control of network elements" (Emphasis added, Barker, column 30, lines 45-46). Further, Barker summarizes his access control features with "the *client based*

access control ... provides a means to restrict access on a *command/client basis*", not at the object level. (emphasis added, Barker, column 31, lines 10-12).

The Examiner cites a passage from Barker (column 23, line 55 – column 26, line 10) describing a set of procedures whereby a client may register to receive notification when managed object attribute values change. The Examiner specifically quotes one line that states, "[n]ote that if more than one attribute has changed for a managed object instance, the changes will be grouped and delivered to each registered client on a managed object instance basis" (Barker, column 26, lines 6-10). Although this portion of Barker teaches clients receiving attribute updates from individual managed objects, and hence object-level notification, it does not teach object-level *access control.* Barker explicitly teaches providing client-based access control at the start of a client session (see Barker, column 30, lines 47-52), while not requiring further authentication or access control based upon which managed objects the client wishes to access.

As the Examiner states, "[e]ach managed object class requires the session identifier as a parameter to each public method" (Barker, column 30, lines 56-58). Applicants assert the session identifier included as a parameter in each public method allows a managed object class to validate the current session – i.e. to ensure that the client has registered with the server and that the session is currently valid. Barker does not teach a client presenting a user name, password or other authentication credentials when registering for object attribute update notification. Instead, Barker teaches that a client must only provide the session ID, object instance identifier, a set of desired attribute codes, and a callback function when registering for attribute update notifications (see Barker, column 25, lines 23-30). Thus, Barker teaches that a managed object class relies upon the server to perform client authentication by just requiring a client to include a valid session identifier in public method calls.

Additionally, Barker teaches that a client can specify a range of managed object instance identifiers, or even *request all instances* in a managed object call through the managed object instance identifier parameter (Barker, column 25, lines 27-28). Hence,

Barker teaches that once a client has been properly authenticated at the start of a session, that client may then register for attribute update notification for a number of managed objects through a single call. Such functionality is clearly not compatible with object-level access control and thus, Barker clearly teaches away from object-level access control, wherein the object-level access control is provided at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects.

In response to the Applicants' previous arguments, the Examiner argues that Barker uses "a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support the IIOP protocol" citing column 8, line 53 – column 9, line 19 and column 7, lines 47-63. Applicants note, however, that these passages of Barker only refer to his use of EMAPI, CORBA, Java, C++, and SNMP, but fail to mention anything regarding any sort of access control for any portion of Barker's system. The Examiner has not cited any particular reference in Barker that describes the features the Examiner is attributing to Barker's system. In fact, the Examiner is incorrectly assuming that Barker's use of CORBA and the IIOP protocol includes object level access control such that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects.

The Examiner also cites Barker teaching, "access permissions associated with the session are examined before authorizing client execution (e.g. remove operation)" (parenthesis in original) (Barker, column 30, lines 58-60). However, this portion of Barker is clearly referring to ensuring that the client has started a valid session with the server. In fact, Barker, referring to the same remove operation, clearly states, "[a]s with any other client requests, the *client must have created a session prior to performing this operation.*" (Emphasis added, Barker, column 22, lines 51-53).

Thus, Applicants assert that Barker does not teach object-level access control between the managers and the managed objects. For at least the reasons given above, the

rejection of claim 1 is not supported by the prior art and its removal is respectfully requested.

Regarding claim 20, the Examiner states, "Barker teaches... wherein the gateway in configured to ... determine on a managed object level whether or not the manager application is allowed to send a request to the managed object as a function of the user of the manager application." Applicants disagree with the Examiner's interpretation of Barker and submit that Barker fails to anticipate determining on a managed object level whether or not the manager application is allowed to send a request to the managed object. In contrast, as shown in the arguments regarding claim 1 above, Barker discloses a method of client based access control of network elements as a means to restrict access on a command/client basis.

Barker further teaches the use of a single service object "to provide services for a class of managed objects" (Barker, column 14, lines 42-43) and that the EM server "will implement one application-specific service object for each type of physical or logical resource to be managed" (underlining added) (Barker, column 39, lines 60-62). Applicants assert that access control on a command/client basis while using a single service object for each class of managed object actually teaches away from determining on a managed object level whether or not the manager application is allowed to send a request to the managed object.

For at least the reasons given above, the rejection of claim 20 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 20 apply to claim 39.

Regarding claim 2, Barker fails to teach wherein the gateway is configurable to determine whether each of the managers is authorized to communicate with each of the managed objects. Instead, Barker teaches the use of a single service object "to provide services for a class of managed objects" (Barker, column 14, lines 42-43) and that the EM server "will implement one application-specific service object for each type of

physical or logical resource to be managed" (underlining added) (Barker, column 39, lines 60-62). Applicants assert that access control on a command/client basis while using a single service object for each class of managed object actually teaches away from determining on a managed object level whether or not the manager application is allowed to send a request to the managed object.

Additionally, Barker discloses client based access control that provides a means to restrict access on a command/client basis (Barker, column 31, lines 10-12). Hence, Barker teaches access control based on a command/client basis, not a managed object basis and thus fails to disclose a gateway that is configurable to determine whether each of the managers is authorized to communicate with each of the managed objects.

For at least the reasons given above, the rejection of claim 2 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 2 apply to claims 21, and 40.

Regarding claim 3, Barker fails to teach a gateway that is configurable to authenticate the managers to receive the events from or to send the request to the managed objects as a function of the identity of the managed object as the Examiner asserts. As the Examiner states, Barker teaches the use of basic server authentication, SSL, and web server administration including client name and password for access control (Barker, column 8, lines 31-54). Further, Barker discloses client based access control that provides a means to restrict access on a command/client basis (Barker, column 31, lines 10-12). However, basic server authentication and SSL using client names and password do not infer the authenticating managers as a function of the identity of the managed object. The Examiner, in the Response to Arguments section of the Office action even refers to Barker's system providing authentication "as a function of the identity of the user of the manager application" (See Office Action, page 5, lines 8-9). The Examiner relies upon his assumption that the "concept of the use of a naming service" includes such an authentication feature without citing any passage where Barker describes authentication of managers as a function of the identity of the managed objects.

For at least the reasons given above, the rejection of claim 3 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 3 apply to claims 22, and 41.

In regards to claim 8, Barker fails to teach wherein the managed objects comprise one or more objects *corresponding* to a telephone network, as asserted by the Examiner. In contrast, Barker discloses a system client that is connected to a network element and element management system client *through* a public switched telephone network (Barker, column 3, lines 48-53). Additionally, Barker teaches the use of a telephone system network through the computer internet and a telephonic link for a system client to connect to the system server (Barker, column 3, lines 54-62). The Examiner argues that Barker's use of the phrase "network elements of a telecommunication network" (See, Barker, Title, and brief descriptions of FIG 1A, 1B, and 1C, column 2, lines 50-65) infer that one or more of Barker's network elements correspond to a telephone network. Applicants submit, however, that Barker is referring to network element residing *on a telecommunications network.* For instance, when discussing FIG. 1B, Barker describes his system as a "method for managing the network element 14 *in* a telephonic network" and continues, "[n]etwork element 14 is connected *through* a telephonic computer network 35 to a computer internet 36" (emphasis added, Barker, column 3, lines 53-58). Hence, Barker discloses *using* a telephonic connection between clients and servers but fails to disclose anything regarding managed objects comprising one or more objects corresponding to a telephone network. None of the managed objects in Barker correspond to a telephone network themselves, but instead communicate using a telephone network. Thus, Barker does not teach wherein the managed objects comprise one or more objects corresponding to a telephone network.

For at least the reasons given above, the rejection of claim 8 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 8 apply to claims 27, and 46.

Regarding claim 10, the Examiner contends that Barker teaches a gateway that is configurable to provide security audit trails. Applicants disagree with the Examiner and submit that at the Examiner's cited passage (Barker, column 17, line 27 – column 18, line 67) Barker only refers to auditing when describing the clean up of filters for a removed client session. For instance, Barker states, "when the Client Session Manger removes a session and/or application from its internal structures, it notifies the Event Distributor via a callback, at which point the Event Distributor removes all filters associated with the session and/or application" (Barker, column 18, lines 10-18). Thus, Barker refers to active Auditing of client sessions to facilitate clean up of event filter lists, but does not include anything about providing security audit trails.

Therefore, the rejection of claim 10 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 10 apply to claims 29, and 48.

In regards to claim 11, Barker fails to teach the gateway providing security audit trails comprises the gateway providing access to a logging service. As shown in the arguments above regarding claim 10, Barker fails to teach a gateway providing security audit trails. Barker also fails to teach the gateway providing security audit trails comprises the gateway providing access to a logging service. The Examiner cites passages referring to individual components of Barker's system storing lists of events to storage devices (Barker, column 11, lines 18-60, column 17, line 33-column 18, line 89, and column 41, line 63 – column 42, line 53). However, Applicants submit that individual components using storage devices to maintain their own lists of data does not equate to a gateway providing access to a logging service.

For at least the reasons given above, the rejection of claim 11 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 11 apply to claims 30, and 49.

Regarding claim 12, the Examiner contends that Barker teaches, "the logging service (local data services at the server) is operable to log an ID of a user that sends each request" (parenthesis and underlining in original). Applicants respectfully disagree with the Examiner's interpretation of Barker. The Examiner cites the same passage cited in regards to the rejection of claim 11 above, but Applicants note that these passages merely refer to the fact that Barker's system includes the ID of a client application when registering event filters for that client application. However, such use of the client application ID does not infer that Barker provides access to a logging service operable to log an ID of a user that receives each event or sends each request. Instead, Barker teaches that his Event Distributor provides an IDL interface for registering filters based in part on an application ID (Barker, column 17, lines 28-30).

Thus, for at least the reasons given above, the rejection of claim 12 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 12 apply to claims 31, and 50.

Regarding claim 18, Barker fails to anticipate wherein requests are converted from the interface definition language to a Portable Management Interface (PMI) format prior to delivery to the managed objects. Instead, Barker teaches, "SNMP Mediator 160 provides translation between the MIB ASN.1 format and the managed object notation used in this architecture" (Barker, column 11, lines 39-42). The Examiner cites a passage where Barker notes that new managed objects could be added (to his system) that utilize a different protocol and encapsulate that knowledge in the managed object class (Barker, column 22, lines18-20). However, Barker fails to mention the PMI format. The Examiner is apparently arguing that by simply stating that other formats may be used, Barker is specifically anticipating every other possible format, including PMI. This is clearly an incorrect interpretation of Barker's teachings. Therefore, Applicants submit that Barker fails to teach that the requests are converted from the interface definition language to a Portable Management Interface (PMI) format prior to delivery to the managed objects as contended by the Examiner.

Thus, the rejection of claim 18 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 18 apply to claims 37, and 56.

Regarding claim 19, the Examiner states, "Barker teaches ... the requests are converted from the interface definition language to a platform-specific format prior to delivery to the managed objects," citing Barker's SNMP mediator providing translation between the MIB ASN.1 format and the managed object notation used in this architecture. Applicants respectfully disagree with the Examiner's interpretation of Barker.

Barker teaches the use of SNMP as the communication protocol between element management system and the managed elements (Barker, column 4, lines 43-45). Applicants assert the SNMP is not a platform-specific format, but rather is a network protocol that contains no platform specific features. Thus, Barker fails to teach the requests are converted from the interface definition language to a platform-specific format prior to delivery to the managed objects as asserted by the Examiner.

For at least the reasons given above, the rejection of claim 19 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 19 apply to claims 38, and 57.

Applicants also assert that numerous other ones of the dependent claims recite further distinctions over the cited art. However, since the independent claims have been shown to be patentably distinct, a further discussion of the dependent claims is not required at this time.

Added Claims:

In a facsimile communication dated May 25, 2004, the Examiner suggests two possible limitations, either of which, if incorporated into Applicants' independent claims, would overcome the prior art and render them in a condition for allowance.

Correspondingly, new claims 58-60 represent claims 1, 20, and 39, respectively, and include the first of the Examiner's suggested additions, namely, "wherein managers use a request SAP for requests and responses." Additionally, new claims 61-63 represent claims 1, 20, and 39, respectively, and include the second of the Examiner's suggested additions, namely, "wherein the gateway uses a singleton SAP object that shares al ProxyAgents through which a manager deals with a managed object and allows the insertion of the user name in the request message to enforce object-level access control." Applicants assert that new claims 58-63 are in condition for allowance as expressed by the Examiner in the May 25, 2004 facsimile.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicants hereby petition for such extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-48400/RCK.

Also enclosed herewith are the following items:

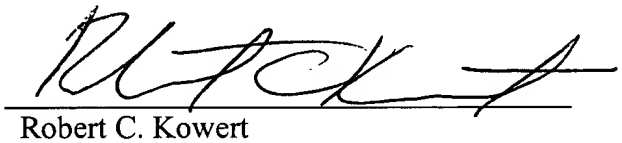
☒ Return Receipt Postcard

☐ Petition for Extension of Time

☐ Notice of Change of Address

☒ Other: Information Disclosure Statement with accompanying Form PTO-1449 and references C1-C17.

Respectfully submitted,



Robert C. Kowert
Reg. No. 39,255
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: October 11, 2004